TITLE 114A
JOINT LEGISLATIVE RULE
SECRETARY OF THE DEPARTMENT OF HEALTH AND HUMAN RESOURCES, INSURANCE COMMISSIONER, AND THE CHAIR OF THE HEALTH CARE AUTHORITY

SERIES 2
ALL-PAYER CLAIMS DATABASE -- PRIVACY AND SECURITY REQUIREMENTS

§114A-2-1. General.

1.1. Scope. -- This joint legislative rule implements the privacy and security provisions of the All Payer Claims Database Program found at W. Va. Code §33-4A-1 *et seq*. as administered by the Department of Health and Human Resources, the Insurance Commissioner, and the Chair of the Health Care Authority.

1.2. Authority. -- W. Va. Code §§33-4A-4(b), (d); 33-4A-8(a) and (e).

1.3. Filing Date. – _____, 2012

1.4. Effective Date. – _____, 2012

§114A-2-2. Definitions.

As used in this joint legislative rule, all terms that are defined in section 1 of the Act and in series 1 of this Title have those same meanings.

2.1. "Act" means the all-payer claims database act, W. Va. Code §33-4A-1 *et seq*.

2.2. "Title" means Title 114A.

§114A-2-3. Data Collection Privacy and Security Requirements.

3.1. Data submitters shall transmit all data to the APCD or its designee over the APCD's secure electronic communications network.

3.2. Transmission of the data from each data submitter to the APCD shall be in a secure manner that prevents unauthorized access and ensures authenticity, confidentiality, and integrity. This data transmission shall be secured to the level required by the HIPAA Security and Privacy Rules, 45 CFR § 164.102 *et seq*. and shall be encrypted per NIST Special Publication 800-52, Guidelines for the Selection and use of Transport Layer Security Implementations, June 2005, NIST Special Publication 800-77, Guide to IPsec VPNs, December 2005, or NIST Special Publication 800-113, Guide to SSL VPNs, July 2008, or others which are Federal Information Processing Standards 140-2, May 2001, validated, all as amended or superseded.

§114A-2-4. Data Retention and Initial Use and Disclosure Privacy and Security Requirements.

4.1. The APCD program shall retain the data in a secure manner that prevents unauthorized access and ensures confidentiality, integrity and availability of all data transmitted to the APCD, at the levels required by the HIPAA Security and Privacy Rules, 45 CFR § 164.102 *et seq*. and shall be encrypted per NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007, as amended or superseded.

4.2. The MOU parties shall only use the data to assess the completeness and quality of data submitters' submissions in order to determine compliance with established data reporting requirements and standards. The MOU parties shall only disclose data back to the respective data submitter, where the completeness and quality review indicates a problem with the data, and such disclosure is required to facilitate the data collection process. For purposes of this initial use, all personal identifiers shall remain encrypted and not visible to the MOU parties. Results of the completeness and quality assessments may be shared with the APCD's Advisory Board.

4.3. No additional uses or disclosures contemplated by this program shall be made until such time as the MOU parties promulgate rules specifically delineating the same.